Fig.1

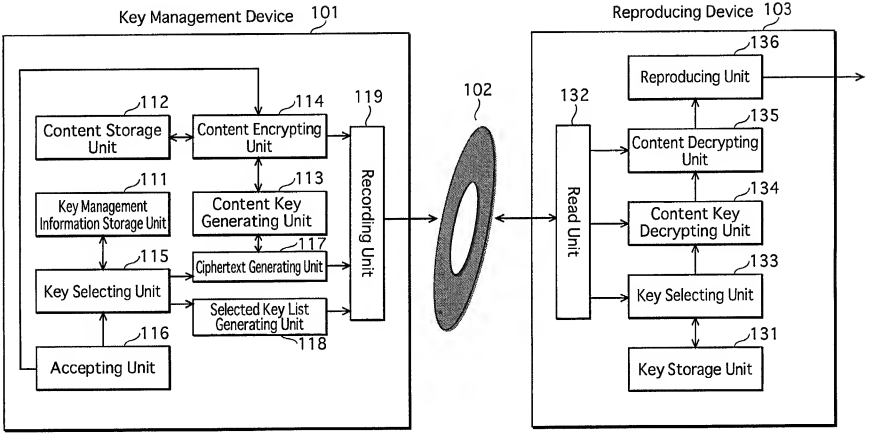

Key Management Device
101
Reproducing Device
103
112
Content Storage Unit
114
Content Encrypting Unit
119
Recording Unit
102
132
Read Unit
136
Reproducing Unit
135
Content Decrypting Unit
111
Key Management Information Storage Unit
113
Content Key Generating Unit
134
Content Key Decrypting Unit
117
Ciphertext Generating Unit
115
Key Selecting Unit
133
Key Selecting Unit
Selected Key List Generating Unit
118
116
Accepting Unit
131
Key Storage Unit

Fig.2

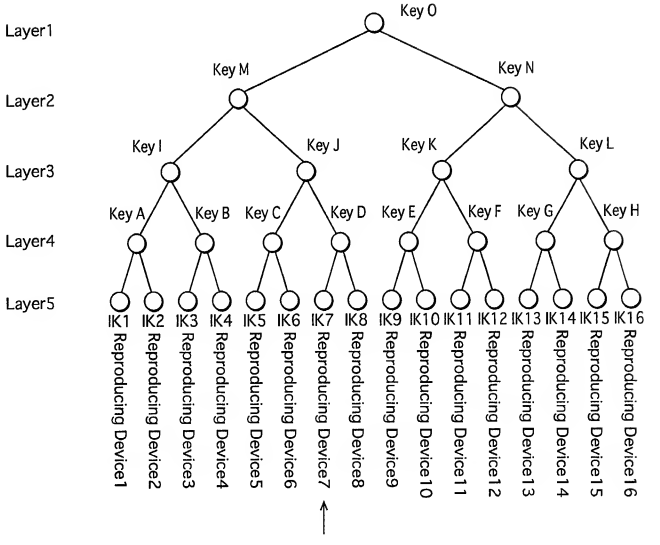

Layer1
Layer2
Layer3
Layer4
Layer5
Key 0
Key M
Key N
Key I
Key J
Key K
Key L
Key A
Key B
Key C
Key D
Key E
Key F
Key G
Key H
IK1 Reproducing Device1
IK2 Reproducing Device2
IK3 Reproducing Device3
IK4 Reproducing Device4
IK5 Reproducing Device5
IK6 Reproducing Device6
IK7 Reproducing Device7
IK8 Reproducing Device8
IK9 Reproducing Device9
IK10 Reproducing Device10
IK11 Reproducing Device11
IK12 Reproducing Device12
IK13 Reproducing Device13
IK14 Reproducing Device14
IK15 Reproducing Device15
IK16 Reproducing Device16

FIG.3

Key Management Information 301

302 Key ID	303 Key Data	304 Parent Key ID	305 Key State
Key 0	・・・・・・・・	11・・・11	1
Key M	・・・・・・・・	Key 0	0
Key N	・・・・・・・・	Key 0	0
Key I	・・・・・・・・	Key M	0
Key J	・・・・・・・・	Key M	0
Key K	・・・・・・・・	Key N	0
⋮	⋮	⋮	⋮
Key A	・・・・・・・・	Key I	0
Key B	・・・・・・・・	Key I	0
Key C	・・・・・・・・	Key J	0
Key D	・・・・・・・・	Key J	0
⋮	⋮	⋮	⋮
IK 1	・・・・・・・・	Key A	0
⋮	⋮	⋮	⋮
IK 7	・・・・・・・・	Key D	0
IK 8	・・・・・・・・	Key D	0
⋮	⋮	⋮	⋮
IK 16	・・・・・・・・	Key H	0

10h121 21Mn1001

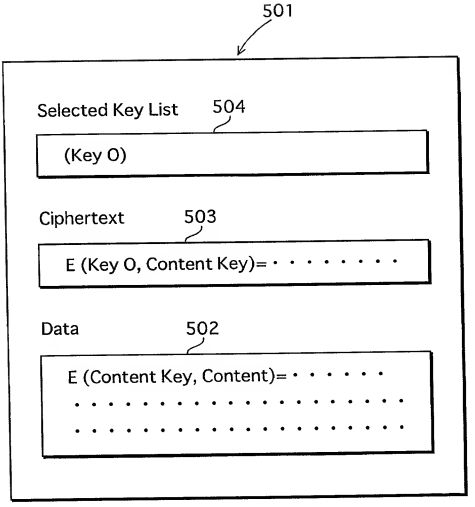
FIG.4

Key Management Information 401

302 Key ID	303 Key Data	304 Parent Key ID	305 Key State
Key 0	・・・・・・・・	11・・・11	-1
Key M	・・・・・・・・	Key 0	-1
Key N	・・・・・・・・	Key 0	1
Key I	・・・・・・・・	Key M	1
Key J	・・・・・・・・	Key M	-1
Key K	・・・・・・・・	Key N	0
⋮	⋮	⋮	⋮
Key A	・・・・・・・・	Key I	0
Key B	・・・・・・・・	Key I	0
Key C	・・・・・・・・	Key J	1
Key D	・・・・・・・・	Key J	-1
⋮	⋮	⋮	⋮
IK 1	・・・・・・・・	Key A	0
⋮	⋮	⋮	⋮
IK 7	・・・・・・・・	Key D	-1
IK 8	・・・・・・・・	Key D	1
⋮	⋮	⋮	⋮
IK 16	・・・・・・・・	Key H	0

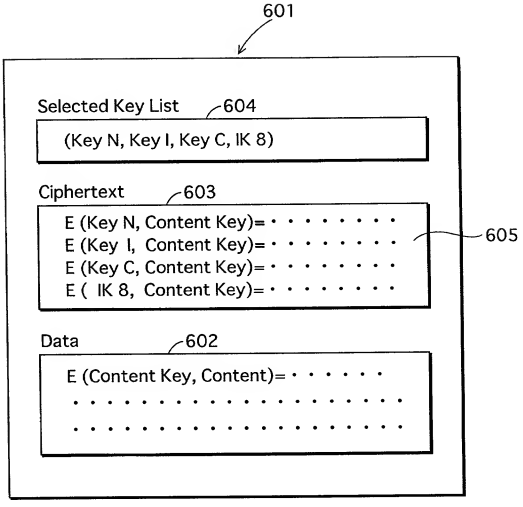
JP2011-216101A 2011.10.27

FIG.5



1001962.1211401

FIG.6



10421-2164P01

FIG.7

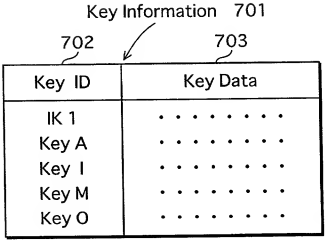

Key Information 701
702
703
Key ID
Key Data
IK 1
Key A
Key I
Key M
Key O

FIG.8

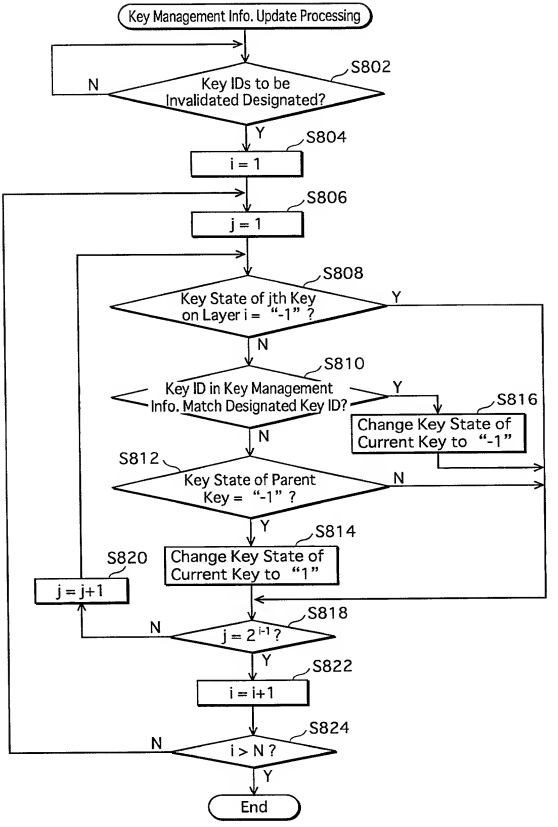

Key Management Info. Update Processing
S802
Key IDs to be Invalidated Designated?
N
Y
S804
i = 1
S806
j = 1
S808
Key State of jth Key on Layer i = "-1" ?
Y
N
S810
Key ID in Key Management Info. Match Designated Key ID?
Y
S816
Change Key State of Current Key to "-1"
N
S812
Key State of Parent Key = "-1" ?
N
Y
S814
Change Key State of Current Key to "1"
S820
j = j+1
N
S818
j = 2^(i-1) ?
Y
S822
i = i+1
S824
i > N ?
N
Y
End

Fig.9

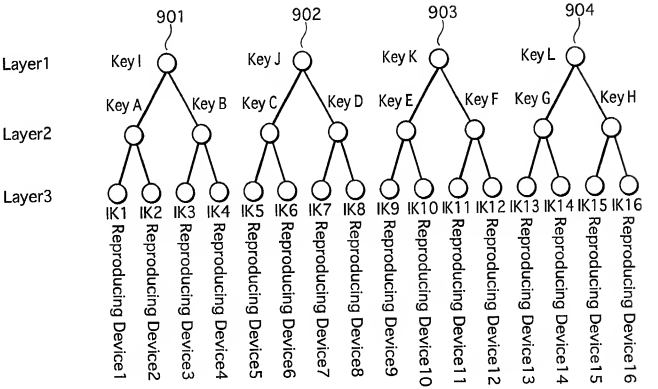

901
902
903
904
Layer1
Layer2
Layer3
Key I
Key J
Key K
Key L
Key A
Key B
Key C
Key D
Key E
Key F
Key G
Key H
IK1 Reproducing Device1
IK2 Reproducing Device2
IK3 Reproducing Device3
IK4 Reproducing Device4
IK5 Reproducing Device5
IK6 Reproducing Device6
IK7 Reproducing Device7
IK8 Reproducing Device8
IK9 Reproducing Device9
IK10 Reproducing Device10
IK11 Reproducing Device11
IK12 Reproducing Device12
IK13 Reproducing Device13
IK14 Reproducing Device14
IK15 Reproducing Device15
IK16 Reproducing Device16

FIG.10

Key Management Information 1001

1002 Key ID	1003 Key Data	1004 Parent Key ID	1005 Key State
Key I	・・・・・・・・	11・・・11	1
Key A	・・・・・・・・	Key I	0
Key B	・・・・・・・・	Key I	0
IK 1	・・・・・・・・	Key A	0
IK 2	・・・・・・・・	Key A	0
IK 3	・・・・・・・・	Key B	0
IK 4	・・・・・・・・	Key B	0
Key J	・・・・・・・・	11・・・11	1
Key C	・・・・・・・・	Key J	0
Key D	・・・・・・・・	Key J	0
IK 5	・・・・・・・・	Key C	0
IK 6	・・・・・・・・	Key C	0
IK 7	・・・・・・・・	Key D	0
IK 8	・・・・・・・・	Key D	0
Key K	・・・・・・・・	11・・・11	1
Key E	・・・・・・・・	Key K	0
⋮	⋮	⋮	⋮
IK 12	・・・・・・・・	Key F	0
Key L	・・・・・・・・	11・・・11	1
⋮	⋮	⋮	⋮
IK 16	・・・・・・・・	Key H	0

10/11/21 21:16:01

FIG.11

Comparison Table 1101

1102 No. of Tree Structures	1103 No. of Keys	1104 No. of Reproducing Devices Misused	1105 No. of Selected Keys =No. of Ciphertexts	1106 No. of Keys Assigned to One Reproducing Device
1	31	0	1	5
		1	4	
		2	6	
2	30	0	2	4
		1	4	
		2	6	
4	28	0	4	3
		1	5	
		2	6	
8	24	0	8	2
		1	8	
		2	8	

10044221 1 2004.01

Fig.12

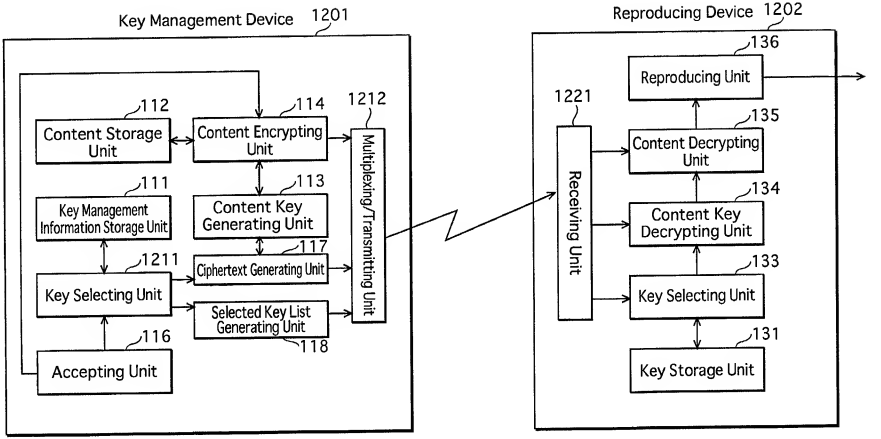

Key Management Device
1201
Content Storage Unit
112
Content Encrypting Unit
114
1212
Multiplexing/Transmitting Unit
Key Management Information Storage Unit
111
Content Key Generating Unit
113
Ciphertext Generating Unit
117
Key Selecting Unit
1211
Selected Key List Generating Unit
118
Accepting Unit
116
Reproducing Device
1202
136
Reproducing Unit
1221
Receiving Unit
Content Decrypting Unit
135
Content Key Decrypting Unit
134
Key Selecting Unit
133
Key Storage Unit
131

FIG.13

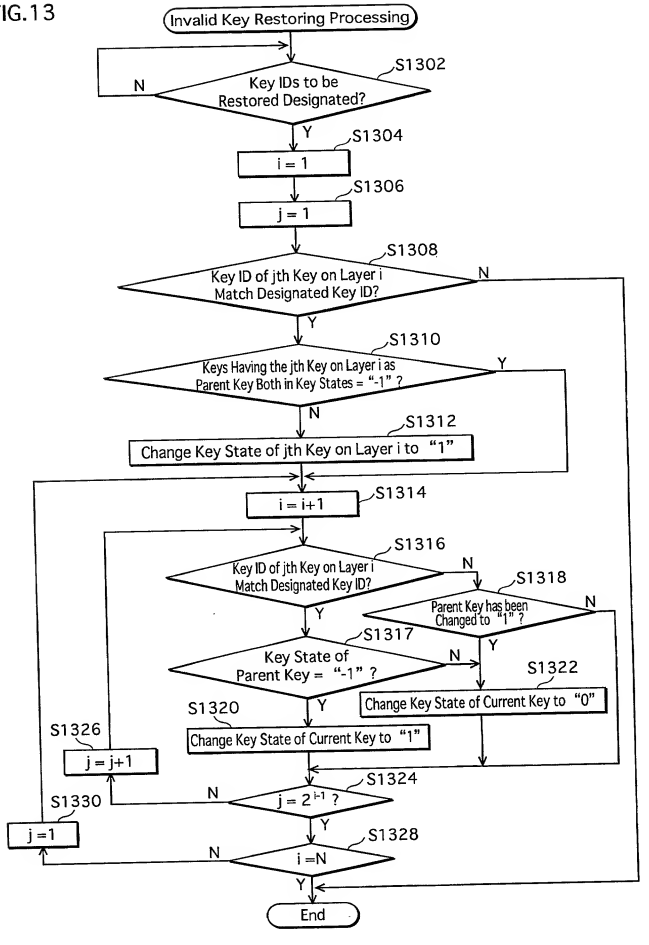

Invalid Key Restoring Processing
S1302
Key IDs to be Restored Designated?
N
Y
S1304
i = 1
S1306
j = 1
S1308
Key ID of jth Key on Layer i Match Designated Key ID?
N
Y
S1310
Keys Having the jth Key on Layer i as Parent Key Both in Key States = "-1" ?
Y
N
S1312
Change Key State of jth Key on Layer i to "1"
S1314
i = i+1
S1316
Key ID of jth Key on Layer i Match Designated Key ID?
N
Y
S1318
Parent Key has been Changed to "1" ?
N
Y
S1317
Key State of Parent Key = "-1" ?
N
Y
S1322
Change Key State of Current Key to "0"
S1320
Change Key State of Current Key to "1"
S1326
j = j+1
S1324
j = 2^(i-1) ?
N
Y
S1330
j =1
S1328
i =N
N
Y
End

Fig.14

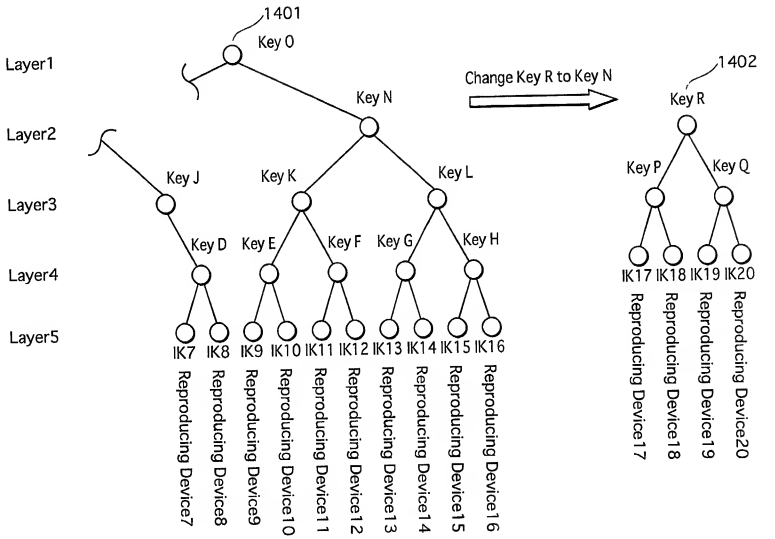

1401
Key 0
Layer1
Key N
Change Key R to Key N
1402
Key R
Layer2
Key J
Key K
Key L
Key P
Key Q
Layer3
Key D
Key E
Key F
Key G
Key H
Layer4
IK17
IK18
IK19
IK20
Reproducing Device17
Reproducing Device18
Reproducing Device19
Reproducing Device20
Layer5
IK7
IK8
IK9
IK10
IK11
IK12
IK13
IK14
IK15
IK16
Reproducing Device7
Reproducing Device8
Reproducing Device9
Reproducing Device10
Reproducing Device11
Reproducing Device12
Reproducing Device13
Reproducing Device14
Reproducing Device15
Reproducing Device16

Fig.15

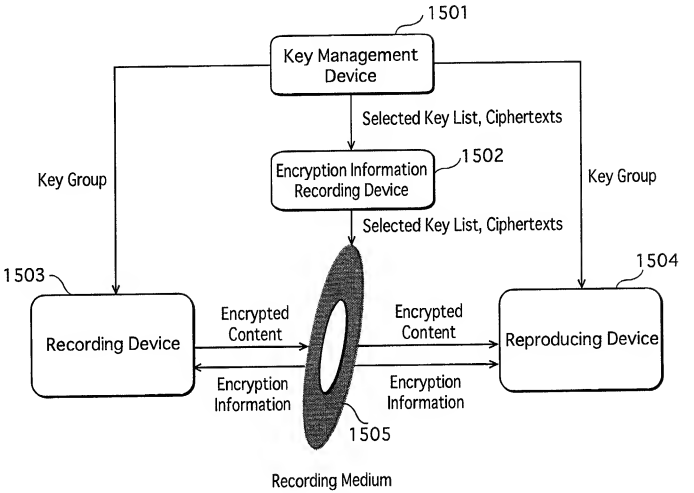

1501
Key Management Device
Selected Key List, Ciphertexts
Key Group
Encryption Information Recording Device
1502
Key Group
Selected Key List, Ciphertexts
1503
1504
Recording Device
Encrypted Content
Encrypted Content
Reproducing Device
Encryption Information
Encryption Information
1505
Recording Medium

Fig.16

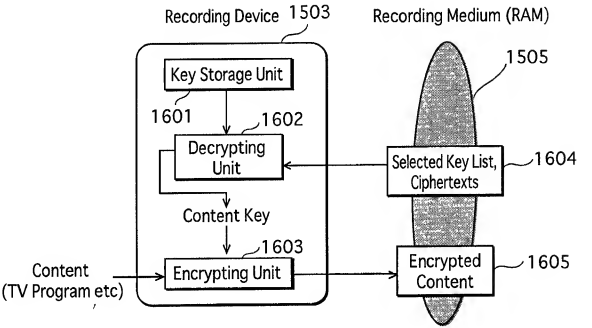
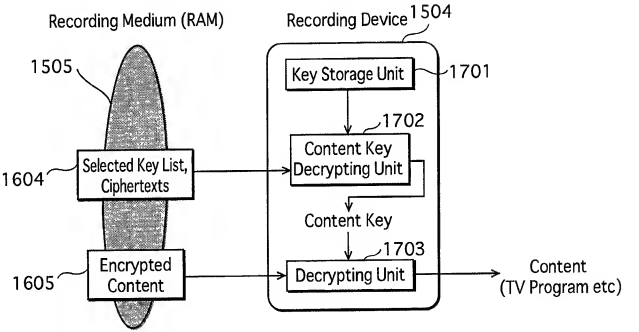

Recording Device 1503
Recording Medium (RAM)
1505
Key Storage Unit
1601
1602
Decrypting Unit
Selected Key List, Ciphertexts
1604
Content Key
1603
Content (TV Program etc)
Encrypting Unit
Encrypted Content
1605

Fig.17


Recording Medium (RAM)
Recording Device
1504
1505
Key Storage Unit
1701
1702
Content Key Decrypting Unit
1604
Selected Key List, Ciphertexts
Content Key
1703
1605
Encrypted Content
Decrypting Unit
Content (TV Program etc)